

UNITED STATES DISTRICT COURT

for the
Eastern District of Missouri

IN THE MATTER OF THE SEARCH OF INFORMATION)
ASSOCIATED WITH THE YAHOO ACCOUNT)
LOVEDOCTOR1984@YAHOO.COM, THAT IS STORED AT)
PREMISES CONTROLLED BY YAHOO INC.)

FILED UNDER SEAL

4:24 MJ 9305 RHH

SIGNED AND SUBMITTED TO THE COURT
FOR FILING BY RELIABLE ELECTRONIC
MEANS

APPLICATION FOR A SEARCH WARRANT

I, Prestyn Atherton, a federal law enforcement officer or an attorney for the government request a search warrant and state under penalty of perjury that I have reason to believe that on the following property:

SEE ATTACHMENT A

located in the _____ District of California, there is now concealed

SEE ATTACHMENT B

The basis for the search under Fed. R. Crim. P. 41(c) is (*check one or more*):

- ☒ evidence of a crime;
☒ contraband, fruits of crime, or other items illegally possessed;
☒ property designed for use, intended for use, or used in committing a crime;
a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

18 U.S.C. § 2251 (production of child pornography), and 2252A(a)(1) & (2) (distribution of child pornography)

SEE ATTACHED AFFIDAVIT WHICH IS INCORPORATED HEREIN BY REFERENCE.

- ☒ Continued on the attached sheet.
☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

I state under the penalty of perjury that the following is true and correct.



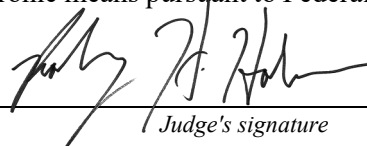
Applicant's signature

Prestyn Atherton, SA, HSI

Printed name and title

Sworn to, attested to, and affirmed before me via reliable electronic means pursuant to Federal Rules of Criminal Procedure 4.1 and 41.

Date: July 23rd, 2024



Judge's signature

City and State: St. Louis, Missouri

Honorable Rodney H. Holmes, U.S. Magistrate Judge

Printed name and title

AUSA: JILLIAN ANDERSON

IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF MISSOURI

IN THE MATTER OF THE SEARCH OF
INFORMATION ASSOCIATED WITH THE
YAHOO ACCOUNT
LOVEDOCTOR1984@YAHOO.COM,
THAT IS STORED AT PREMISES
CONTROLLED BY YAHOO INC.

FILED UNDER SEAL

4:24 MJ 9305 RHH

SIGNED AND SUBMITTED TO THE COURT
FOR FILING BY RELIABLE ELECTRONIC
MEANS

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Prestyn Atherton, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information associated with a certain account that is stored at premises owned, maintained, controlled, or operated by Yahoo Inc (“Yahoo”), an electronic communications service and/or remote computing service provider headquartered at 770 Broadway, 9th Floor, New York, NY 10003-9562. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Yahoo to disclose to the government copies of the information (including the content of communications) further described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

2. I am a Special Agent with the Department of Homeland Security, U.S. Immigration and Customs Enforcement (ICE), Homeland Security Investigations (HSI), and have been since July 2023. I am currently assigned to the HSI office in Saint Louis, Missouri. In that role, I investigate a variety of different federal criminal violations, including federal criminal violations

related to high technology or cybercrime, child exploitation, and child pornography. I completed training on these and related topics through the Federal Law Enforcement Training Center (FLETC), Criminal Investigator Training Program (CITP), Homeland Security Investigations Special Agent Training (HSISAT), and through various in-service trainings offered through my agency and external partners. This training includes the requirement to observe, review, and classify numerous examples of child pornography (as defined in 18 U.S.C. § 2256) in several forms of electronic media. I hold a bachelor's degree with a dual major in Criminal Justice and Management. Moreover, I am a federal law enforcement officer who is engaged in enforcing criminal laws, including 18 U.S.C. §§ 2251, 2252, and 2252A, and I am authorized by law to request a search warrant.

3. The facts in this affidavit come from personal observations, training and experience, and information obtained from other law enforcement and witnesses. This affidavit is merely intended to show sufficient probable cause for the requested warrant and does not set forth all my knowledge about this matter.

4. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of 18 U.S.C. § 2251 (production of child pornography), and 2252A(a)(1) & (2) (distribution of child pornography) were committed by Richard James MILLER. There is also probable cause to search the information described in Attachment A for evidence, instrumentalities, and contraband of these crimes further described in Attachment B.

JURISDICTION

5. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), &

(c)(1)(A). Specifically, the Court is “a district court of the United States . . . that has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i).

6. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

LOCATION TO BE SEARCHED

7. The location to be searched is:

8. Yahoo Account: **lovedoctor1984@yahoo.com** located at a premises owned, maintained, controlled, or operated by Yahoo Inc, a company headquartered at 770 Broadway, 9th Floor, New York, NY 10003-9562.

BACKGROUND CONCERNING EMAIL

9. In my training and experience, I have learned that the Provider provides a variety of on-line services, including electronic mail (“email”) access, to the public. The Provider allows subscribers to obtain email accounts at the domain name sbcglobal.net, like the email account[s] listed in Attachment A. Subscribers obtain an account by registering with the Provider. During the registration process, the Provider asks subscribers to provide basic personal information. Therefore, the computers of the Provider are likely to contain stored electronic communications (including retrieved and unretrieved email for the Provider subscribers) and information concerning subscribers and their use of the Provider services, such as account access information, email transaction information, and account application information. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account’s user or users.

9. In my training and experience, email providers generally ask their subscribers to provide certain personal identifying information when registering for an email account. Such information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative email addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number). In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users. Based on my training and my experience, I know that, even if subscribers insert false information to conceal their identity, this information often provides clues to their identity, location, or illicit activities.

10. In my training and experience, email providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (*i.e.*, session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other log files that reflect usage of the account. In addition, email providers often have records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the email account.

11. In my training and experience, in some cases, email account users will communicate directly with an email service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Email providers

typically retain records about such communications, including records of contacts between the user and the provider's support services, as well as records of any actions taken by the provider or user as a result of the communications. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

12. As explained herein, information stored in connection with an email account may provide crucial evidence of the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, the information stored in connection with an email account can indicate who has used or controlled the account. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. For example, email communications, contacts lists, and images sent (and the data associated with the foregoing, such as date and time) may indicate who used or controlled the account at a relevant time. Further, information maintained by the email provider can show how and when the account was accessed or used. For example, as described below, email providers typically log the Internet Protocol (IP) addresses from which users access the email account, along with the time and date of that access. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the email account access and use relating to the crime under investigation. This geographic and timeline information may tend to either inculcate or exculpate the account owner. Additionally, information stored at the user's account may further indicate the geographic location of the account user at a particular time (*e.g.*, location information integrated into an image or video sent

via email). Last, stored electronic data may provide relevant insight into the email account owner's state of mind as it relates to the offense under investigation. For example, information in the email account may indicate the owner's motive and intent to commit a crime (*e.g.*, communications relating to the crime), or consciousness of guilt (*e.g.*, deleting communications in an effort to conceal them from law enforcement).

13. In general, an email that is sent to the Provider is stored in the subscriber's "mail box" on the Provider's servers until the subscriber deletes the email. If the subscriber does not delete the message, the message can remain on the Provider's servers indefinitely. Even if the subscriber deletes the email, it may continue to be available on the Provider's servers for an extended period of time and, in some circumstances, indefinitely.

PROBABLE CAUSE

10. On March 18, 2024, Homeland Security Investigations (HSI) Cherry Hill, New Jersey executed a search warrant in furtherance of a child exploitation investigation. Your undersigned affiant was briefed about this investigation, including the information set forth below.

11. Upon forensic review of a phone seized during the search warrant, a Kik messenger group chat was identified between the subject of the investigation and two unknown Kik users, "MasterDogg69" and a third user unrelated to this application. The context of the group chat was for like-minded individuals to discuss sexual abuse of family members, including children. In the group chat, "MasterDogg69" shared explicit photographs of girls he claimed were his teenage daughters. The user of the Kik Messenger account "MasterDogg69" states in the chat that he is from Missouri and the abuse began when the children were about 10 years old.

12. On April 10, 2024, HSI Cherry Hill contacted HSI St. Louis regarding Kik user “Masterdogg69” and suspected criminal activity that occurred within the HSI St. Louis Area of Responsibility (AOR), and an investigative referral was sent on April 23, 2024.

Subpoena for Kik Account User “MasterDogg69”:

13. Your undersigned affiant was further informed as follows regarding subpoenas sent to Kik Messenger and Charter Communications by HSI Cherry Hill. On March 27, 2024, HSI Cherry Hill agents sent a DHS summons to Kik c/o MediaLab.ai Inc. regarding username “MasterDogg69” requesting Internet Protocol (IP) addresses and subscriber data associated with the account. On March 28, 2024, Kik provided the following, as well as other, subscriber information and IP address for the user:

Username: Masterdogg69

First name: M. Crazy

Last Name: Dogg69

Email: lovedoctor1984@yahoo.com (confirmed)

Kik provided the following IP address associated with the account for the timeframe of February 28, 2024 – March 26, 2024: 75.133.153.127

Subpoena for Charter Communications for IP 75.133.153.127:

14. On April 4, 2024, HSI Cherry Hill agents sent a DHS summons to Charter Communications, Inc. (hereinafter, “Charter”) for subscriber information and log data for IP address 75.133.153.127 for March 4, 2024, during the time the Kik account “MasterDogg69” was actively sending messages and images on the group chat. Charter provided subscriber information and log data for the timeframe of February 28, 2024-March 26, 2024, for that IP address which showed service address: 1100 N SAINT JOE DR, APT 21, PARK HILLS, MO 63601-1944.

Identification of Richard MILLER

15. Government and commercial databases link 1100 North Saint Joe Drive, Unit 21, Park Hills, Missouri 63601 (hereinafter “MILLER’S RESIDENCE”) to Richard James MILLER (DOB: 10/04/1984). A U.S. Department of Housing and Urban Development (HUD) Office of Inspector General (OIG) Special Agent (SA) confirmed that MILLER received HUD assistance at that address, a single bedroom apartment located within the St. Francis Heights Apartments complex. Missouri Department of Revenue records show MILLER’s RESIDENCE on his State Identification card.

Review of Kik Group Chat:

16. Your undersigned affiant reviewed the Kik group chat digital evidence discovered by HSI Cherry Hill during the execution of a search warrant in their investigation, wherein I observed Kik user “Masterdogg69” in a chat with two other users, discussing incestual fantasies and sharing stories of incest/sexual abuse. Kik user “MasterDogg69” distributed multiple image files that appear to depict pubescent females engaged in sexually explicit conduct, which “MasterDogg69” stated were his 18 and 16-year-old daughters. “MasterDogg69” stated that he began sexually abusing the girls when they were 10 years old. The following is a summation of content I observed in the chat. All the messages summarized below were sent on March 4, 2024, between 1:47 PM and 8:19 PM.

17. “MasterDogg69” stated that he was from Missouri.

18. “MasterDogg69” stated that he regularly engages in sexual intercourse with who he claimed is his then 16-year-old and 18-year-old daughters. “MasterDogg69” stated that he believed his daughters were 10 years of age when he started sexually abusing them.

19. “MasterDogg69” stated, “My other will be 17 tomorrow, which is legal in my state” referring to his youngest daughter and offered to send pictures of her to the other users in the chat.

20. “MasterDogg69” distributed several image files that depicted what appears to be a pubescent female, which the user claimed was his 16-year-old daughter, completely nude with lascivious display of her genitals and engaged in masturbation. One image depicts the nude lower half of a female’s body sitting in a bathtub. Two other images depict what appear to be a video thumbnail of the nude lower half of a female engaged in masturbation in a bathtub. In another image file sent, a fully nude female is standing in front of a mirror taking a selfie. Her face and genitals are visible.

21. “MasterDogg69” sent an image file of what appears to be a video thumbnail of a female, which he claimed to be his 16-year-old daughter, engaged in sex with a male and stated, “This me and her fucking in her pussy.”

22. Another user in the chat stated that it looks like “MasterDogg69” has consensual and non-consensual sex whenever he wants with the females and “MasterDogg69” responded, “Exactly.” “MasterDogg69” later stated “I get what I want when I want mainly they love it that way.”

23. “MasterDogg69” distributed image files depicting what appears to be a pubescent female engaged in sexually explicit conduct, which he stated was his now 18-year-old daughter. In one image, there is a man engaged in what appears to be oral sex on a female and half of the man’s face is visible. The hair, facial hair, and other facial features of the man are generally consistent with the individual depicted in the photograph on Richard MILLER’s Missouri state identification card and the adult male your undersigned affiant saw enter MILLER’S RESIDENCE while conducting surveillance on May 3, 2024. In the background of 2 images, a dark stained wood

door can be seen that appears to be the same door in the background of other pictures sent by “MasterDogg69”.

24. “MasterDogg69” sent two other image files of females engaged in sexually explicit conduct with a man and claimed they were of his “other oldest” and his sister. Half of the man’s face is visible, and his facial hair and other facial features are generally consistent with that of a man your undersigned affiant observed enter the MILLER’S RESIDENCE while conducting surveillance on May 3, 2024, and the individual depicted in the photograph on Richard MILLER’s Missouri state identification card. In the background of the image, a dark stained wood door can be seen that appears to be the same door in the background of other pictures sent by “MasterDogg69”.

Execution of Search Warrant at MILLER’S RESIDENCE

25. On May 24, 2024, your undersigned affiant applied for and received federal criminal search and seizure warrant No. 4:24 MJ 6106 PLC from the United States District Court for the Eastern District of Missouri for MILLER’S RESIDENCE. On June 4, 2024, HSI Special Agents and local law enforcement executed the search and seized two (2) laptop computers and three (3) cellular phones and took photos of the interior of the apartment which matched those in the background of the child exploitation images distributed by MILLER on Kik. In particular, the above-mentioned dark wood-stained door and white closet door in the bedroom of MILLER’s apartment, as well as what can be described as Native American artifacts hanging on the wall, all of which can be seen in the background of photos sent by MILLER in the Kik chat.

Interview of MILLER

26. Concurrent with execution of the residential search warrant Special Agents interviewed MILLER. In a post warned statement MILLER admitted he used the Kik application under username mistercrazywolf or mcrazywolf69 and, after being shown chat transcripts, also confirmed he may have used the username MasterDogg69. MILLER stated he thought his Google account was whitedogg69@gmail.com and later stated it may be whitedogg1956@gmail.com. MILLER confirmed that there should be three (3) cellular phones in his apartment, two (2) of which (described as a Samsung and Vortex Phone) belong to him and one (1) of which (described as a blue TracFone) belongs to a minor victim with initials LR (hereinafter referred to as "MV1"). MILLER confirmed there should be two (2) laptop computers (described as HP and Lenovo) which belong to him. All five (5) devices were found in the residence and seized as evidence.

27. MILLER admitted to receiving and accidentally clicking on a link to download child pornography on Kik the day prior, June 3, 2024, using account username mcrazywolf69.

28. MILLER admitted to engaging in sexual intercourse and oral sex with MV1, recording/photographing it, and then distributing the explicit images of her to other users on Kik messenger. MILLER stated he distributed the images as recently as the evening of June 3, 2024. MILLER confirmed that he has knowledge that MV1 is 17 years of age and stated he thought she was 17 years of age at the time the videos/photos were taken. MILLER was shown a transcript of the above described Kik chat and confirmed that he was the author of the chat, was using Kik username MasterDogg69, and that some of the images/videos he distributed were videos he produced of himself and MV1 nude and engaged in sexual intercourse. MILLER stated that he

refers to MV1 as his “daughter,” although they are not related. MILLER stated that he has known and spent time with MV1 for 3 years.

29. MILLER admitted to engaging in sexual intercourse with a second female with the initials KS (hereinafter “MV2”), whom he stated he thought was 19 years of age, recording/photographing it, and then distributing the explicit images of her to other users on Kik. MILLER was shown the portion of the above mentioned Kik chat transcript and confirmed that MV2 is one of the females depicted in the images on the chat engaged in oral sex, sexual intercourse, and lascivious display of the genitals and that he produced the images. MILLER stated he thought she was 18 years of age at the time of the chat. MILLER stated that he would refer to her as his “daughter” even though they are of no relation.

30. Upon review of the rest of the explicit images distributed in the Kik chat, MILLER stated that the other females depicted in the images were of a mother and daughter from another state who came to visit and have sex “a while ago.” He claimed that the daughter is going to be graduating high school this year. He later denied having sex with them and stated that the mother sent him the images.

Interview of Minor Victim One (1)

31. On June 6, 2024, a HSI Forensic Interview Specialist (FIS) interviewed a minor victim associated with this case with the initials LR (hereinafter referred to as “MV1”). MV1 stated she is 17 years of age and that she was 15 years of age when she first met MILLER and began spending time at his apartment. MV1 stated she engaged in oral sex and sexual intercourse with MILLER on multiple occasions starting when she was 15 years of age. MV1 stated he would use

sex toys described as a vibrator, dildo, handcuffs, ball and chain, collar with leash, and strawberry flavored lube on her and two other juvenile females. MV1 stated that MILLER would sometimes force her and two other juvenile females, one of which she thought to be 9 years of age and the other 17 years of age at the time of the abuse, to have sex or engage in oral sex with him. MV1 stated that MILLER would use his cell phone to photograph and record her, and the other juveniles, fully nude and while engaging in sexually explicit conduct. MV1 stated MILLER would manipulate or force her to send him photographs and videos of her nude and engaged in masturbation and threatened to hurt MV1's dad if she told anyone or stopped. MV1 state that MILLER would distribute the pornographic photographs and videos of her to other users on Kik Messenger and would show her the chat and the other users' responses to the images. MV1 stated that MILLER would often refer to her as his "daughter." MV1 was shown pictures of the above-described explicit images sent on Kik by MasterDogg69 described as "Pictures 1-6". MV1 confirmed that the images were of her when she was 16 years of age and that the username used to distribute them (MasterDogg69) was a username she recognized as one used by MILLER on Kik. It should be noted that MV1 confirmed that one of the video thumbnails described above, which MILLER stated in the chat was him engaging in sex with his 16-year-old daughter and labeled in this interview as "Picture 4," was a video of MV1 and MILLER engaged in sexual intercourse. MV1 stated she also observed MILLER use a username which she thought to be mcrazywolf69 to distribute images/videos of her on Kik. MV1 also stated that she would send explicit images to MILLER via Snapchat username whitedogg1956, display name "White Dogg69" and MILLER would send explicit images of himself to her.

Interview of Victim Two (2)

32. On June 6, 2024, the FIS interviewed a victim associated with this case, described above by MV1 as the 17-year-old juvenile female, with the initials KS (hereinafter referred to as “KS”). KS stated she is 19 years of age and that she was 17 years of age when she first met MILLER and began spending time at his apartment. KS stated that she engaged in sexual intercourse and oral sex with MILLER multiple times starting when she was 17 years of age. KS stated she witnessed MV1 and MILLER have sexual intercourse and oral sex when MV1 was 15 years of age. KS stated that MILLER recorded both MV1 and herself engaged in sexually explicit conduct and distributed the images to other users on Kik. KS stated that MILLER would request sexually explicit videos/photographs of her genitals and engaged in masturbation and would then distribute those videos to other users on Kik and show her the chat. KS was shown the explicit images suspected to be of her distributed by MILLER in the above-mentioned chat and she confirmed that it was her and MILLER depicted in the images. KS stated that she would also send explicit images of herself to MILLER’s snapchat username whitedogg1956. KS stated that MILLER showed her a video on his cell phone of a “little boy,” whom she thought to be a young child, having sex with a grandma. KS stated that MILLER had multiple phones. KS stated that MILLER would use the above-mentioned sex toys on both her and MV1.

Interview of Minor Victim Three (3)

33. On June 6, 2024, the FIS interviewed a minor victim associated with this case, identified as one of the female juveniles described above by MV1, with the initials KS (hereinafter referred to as “MV3”). MV3 stated she is 10 years of age and that she first met MILLER and began spending time at his apartment approximately 2 years ago. MV3 stated that her dad and MILLER

were good friends and that their family stayed at MILLER's apartment for a period of time when they were homeless. MV3 stated that MILLER and MV1 had sex in front of her. MV3 stated that MILLER touched her thighs inappropriately and showed her pornographic videos, including that of bestiality. MV3 stated she saw MILLER and MV1 use the above-mentioned sex toys in front of her. MV3 stated she knew MILLER recorded/photographed MV1 and MV2 engaged in sexually explicit conduct and sent the images on the internet. MV3 stated she was not comfortable stating anymore because she was afraid her mother would be mad at her.

Review of Devices Seized During Search Warrant

34. As a result of the search warrant executed on June 4, 2024, three (3) cellular phones and two (2) laptops were seized from MILLER's residence. Forensic examination of the devices seized from the residence is ongoing, but I observed artifacts of Kik usernames Masterdogg69 and mcrazywolf69 and Google account whitedogg1956@gmail.com suggesting use by and attribution to MILLER across multiple devices seized from the residence.

35. A manual and forensic review of the device described as a Vortex HD65 Plus Android Cell phone, IMEI 359525842487038 (hereinafter "Vortex Phone"), which MILLER stated was his device, provided the correct passcode for, and gave a matching phone number for, revealed the presence of Child Sexual Abuse Material. Explicit photographs of the above mentioned MV1, MV2, and MV3 engaged in lascivious display of the genitals, sexual intercourse and masturbation were found on the device, including the above-described images sent in the Kik chat. There are multiple images of MV3 engaged in lascivious display of the genitals and sexual intercourse in what appears to be MILLER's apartment bedroom. The same room décor, painting, dark wood-stained doors, and white closet door, which is in MILLER's apartment bedroom can

be seen in the background of the explicit images of MV3. Numerous other explicit videos and photos of age-difficult, unidentified females were also found on the device.

36. The Vortex Phone was logged into and linked to automatically sync and backup to Google account: whitedogg1956@gmail.com. Sexually explicit video thumbnails could be seen stored in the Google account, but since the forensic and manual review of the device is done in “airplane mode” (not connected to the internet), the videos would not play and a search warrant for the Google account was needed to further access that data. On June 21, 2024, search warrant No. 4:24 MJ 3211 NCC was signed and executed on Google for account information pertaining to whitedogg1956@gmail.com.

The Subject Yahoo Account

37. On June 26, 2024, Google LLC provided responsive records for account whitedogg1956@gmail.com under Google Reference Number 63140615. Review of that material is ongoing, but revealed artifacts indicating distribution or receipt of known child pornography, and other suspected child pornography, between whitedogg1956@gmail.com and SUBJECT ACCOUNT lovedoctor1984@yahoo.com. For example:

38. On April 25, 2024, whitedogg1956@gmail.com sent a child pornography image of MV1 in an email attachment to lovedoctor1984@yahoo.com. The image depicts MV1 taking a mirror selfie while fully nude with lascivious display of the genitals. The following are the identifiers for the child pornography image file:

- a. MD5 Hash: e795fcddb1c48ab64f5a4094f0eb839d, File Name: received_404287988919037.jpeg, and email subject line: “[MV1’s First Name], Sarah, Anna bell, and Rachel.”

39. lovedoctor1984@yahoo.com is the email account linked to the above-described Kik account with username MasterDogg69, which sent/received child pornography of the above-identified MV1 and which this affidavit lays out attribution to Richard MILLER. It should be noted that 1984 is MILLER’s year of birth and the name associated with the email account is “Richard Miller.”

INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

40. Your undersigned affiant anticipates executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require Yahoo to disclose to the United States copies of the records and other information (including the content of communications and stored data) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

CONCLUSION


41. Based on the forgoing, your undersigned affiant request that the Court issue the proposed search warrant. The United States will execute this warrant by serving the warrant on Yahoo. Because the warrant will be served on Yahoo, who will then compile the requested records

at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

42. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

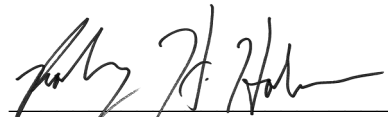
43. I further request that the Court order that all papers in support of this application, including the affidavit and warrant, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may give targets an opportunity to flee/continue flight from prosecution, destroy or tamper with evidence, change patterns of behavior, notify confederates, or otherwise seriously jeopardize the investigation.

I state under the penalty of perjury that the foregoing is true and correct.



Prestyn Atherton
Special Agent
Homeland Security Investigations

Sworn to, attested to, or affirmed before me via reliable electronic means pursuant to Federal Rules of Criminal Procedure 4.1 and 41 on this 23rd day of July, 2024.



HON. RODNEY H. HOLMES
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

4:24 MJ 9305 RHH

Property to Be Searched

This warrant applies to information associated with **lovedoctor1984@yahoo.com** that is stored at premises owned, maintained, controlled, or operated by Yahoo Inc a company headquartered at 770 Broadway, 9th Floor, New York, NY 10003-9562.

ATTACHMENT B

4:24 MJ 9305 RHH

Particular Things to be Seized

I. Information to be disclosed by Yahoo Inc. (the “Provider”)

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, regardless of whether such information is located within or outside of the United States, and including any emails, records, files, logs, or information that has been deleted but is still available to the Provider, the Provider is required to disclose the following information to the government for each account or identifier listed in Attachment A:

- a. The contents of all emails associated with the account from June 1, 2014, to present, including stored or preserved copies of emails sent to and from the account, draft emails, the source and destination addresses associated with each email, the date and time at which each email was sent, and the size and length of each email;
- b. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);
- c. The types of service utilized;
- d. All records or other information stored by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, and files; and

e. All records pertaining to communications between the Provider and any person regarding the account, including contacts with support services and records of actions taken. The Provider is hereby ordered to disclose the above information to the government within 14 days of issuance of this warrant.

II. Information to be seized by the United States

All information described above in Section I that constitutes contraband, evidence, and instrumentalities of violations of 18 U.S.C. § 2251, 2252A(a)(2), and (a)(5)(B), those violations involving Richard MILLER and occurring from at least as early as June 1, 2014, to Present, including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

14. The production, purchase, receipt, or possession of child pornography or attempts to commit, including any such contraband material stored within cloud storage or as attachments to messages, even when deleted or marked for deletion;
15. Evidence indicating how and when the Account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the email account owner;
16. Evidence indicating the Account owner's state of mind as it relates to the crime under investigation;
17. The identity of the person(s) who created or used the Account, including records that help reveal the whereabouts of such person(s).
18. The identity of the person(s) who communicated with the Account about matters relating to receipt and distribution of child pornography, including records that help reveal their whereabouts.